(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 December 2000 (14.12.2000)

PCT

(10) International Publication Number
WO 00/76215 A1

(51) International Patent Classification[7]: H04N 7/16, G07F 7/10

(21) International Application Number: PCT/IB99/01213

(22) International Filing Date: 4 June 1999 (04.06.1999)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: OPEN TV, INC. [US/US]; 401 East Middlefield Road, Mountain View, CA 94043 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: DELPUCH, Alain [FR/FR]; 34, parc des Essarts, F-78690 Les-Essart-le-Roi (FR).

(74) Agents: BENECH, Frédéric et al.; 69, avenue Victor Hugo, F-75783 Paris Cedex 16 (FR).

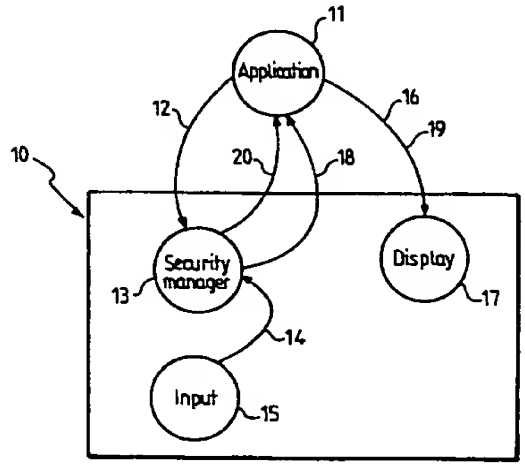
(81) Designated States *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: FLEXIBLE INTERFACE FOR SECURE INPUT OF PIN CODE



(57) Abstract: The present invention concerns a system (10) and a process for authenticating a PIN code of a user in an interactive information system in order to run an application. It comprises input means (15) for PIN code entry, security manager means (13) for comparing the PIN code of the user upon a request for user authentication from the application, with a registered PIN code, and giving authorisation to run said application if the PIN code of the user matches with the registered PIN code, and display means (17) for displaying any graphics including a PIN entry field. The request for user authentication is provided on the display means via the PIN entry field with the look and feel of said application. The system further comprises emitting means for entering crypted digits, the security manager means (13) being arranged to give authorisation to run the application after full entry of said crypted digits and if the PIN code of the user is identical to the registered PIN code.

WO 00/76215 A1

FLEXIBLE INTERFACE FOR SECURE INPUT OF PIN CODE

The invention is related to interfaces between man and machine such as computer, telephone or television devices, which need a Personal Identification Number (PIN) to authenticate the user running an application.

By running an application, one should understand to continue or to have access to an application or to specific resources of an application.

The invention is more particularly but not exclusively related to a system and a method used in an interactive information system such as an entertainment system.

Requirements for security in interactive entertainment systems are contradictory.

This is because, in order to run an application, an authentication of the user/viewer is needed while using the specific look and feel of the application.

However, it is also preferred that the PIN code should not be given to the application for security purpose.

In fact, two types of solutions are presently known for authentication. Both present drawbacks, as they are only capable of fulfilling part of the above requirements.

Either the application presents its own user interface for PIN entry, then queries the underlying system to check if the given PIN is correct.

This solution does not hide the PIN code from the application.

Or the application requests the underlying system to authenticate the viewer. For this the underlying system, using its own look and feel, prompts the viewer for its PIN, verifies its validity and then returns the information that the viewer is authorised or not to the application.

This solution is safe, but does not allow integration of the PIN entry with the application look and feel.

In other words and referring to figure 1, it is shown a system which presents a good look and feel , but which is not safe, as the PIN code is known by the application.

More precisely, the application 1 has total control of the look and feel.

The viewer provides his PIN code through input means 2 in digital data to the application via an input device, for instance transmitted as infrared signals 3 to the device on which runs the application which displays in 4 the look and feel for the PIN entry field.

Such application, which is now aware of the PIN code, transmits it in 5 to security manager means 6 which, after checking, confirms in 7 authorisation from the system 8.

The PIN code (Input means 2) is therefore provided outside of the system 8, which is unsecured, and may allows third parties to have access to the PIN code.

Figure 2 displays the other way of functioning of a known system of the prior art.

Here, the application 1 has no control over the look and feel, contrarily to the precedent case.

The application 1 requests in 9 the system 8 to identify the user.

The security manager means 6 uses the input means 2 (PIN Code), provided in 3 and the display screen to create in 4 a display of the PIN entry field.

When the security manager means 6 has checked the PIN code, it gives authorisation (7) to display or to access to resource to the application 1.

On a security point of view this system is good as, at no point, the system 8 gives out the PIN code to the application.

However, the look and feel is here totally under system control, without any consideration for the current application look and feel.

It is therefore a main object of the present invention to provide an improved system and method for authorising a secure way of authentication for an access to an application through a PIN code while using the look and feel of said application during the PIN code interrogation.

It is another object of the invention to provide an improved system and method wherein the safety needed for PIN code entry, is combined with perfect integration of the prompt with the service.

It is another objet of the invention to provide a simple and cost saving flexible interface for secure input of a PIN code.

The problems outlined above are in large part solved by a system for authenticating a PIN code of a

user in an interactive information system, in order to run an application which comprises :

- input means for PIN code entry,
- security manager means for comparing the PIN code of the user, upon a request for user authentication from the application, with a registered PIN code, and giving authorisation to run said application if said PIN code of the user matches the registered PIN code,
- and display means for displaying any graphics including a PIN entry field,

characterised in that

the request for user authentication being provided on the display means via the PIN entry field with the look and feel of said application, the system further comprises emitting means for entering crypted digits in said PIN entry field upon entering the PIN code of the user in the security manager means through said input means,

and the security manager means are arranged to give authorisation to run the application after full entry of said crypted digits and if the PIN code of the user is identical to the registered PIN code.

With such system the PIN code remains hidden from the environment, the user having only the impression to enter physically his PIN code within the PIN entry field of the application. In fact, it remains in the security manager means, which is within the system.

In a preferred embodiment the application is a television program.

The invention also provides a method for authenticating a PIN code of a user in an interactive information system, in order to run an application,

wherein said information system emits a request for authenticating a user,

said user enters a PIN code through input means,

said PIN code of the user is compared with a registered PIN code, within security manager means,

and authorisation is provided to run said application if the PIN code of the user matches with the registered PIN code,

characterised in that

- the request for authenticating being provided with a PIN entry field having the look and feel of the application,
- crypted digits are entered in said PIN entry field, upon entering the PIN code by the user in the security manager means,

and authorisation to display the application is only provided after full entry of said crypted digits, and if the PIN code signal of the user is identical to the registered PIN code as checked by the security manager means.

The invention will be better understood from reading the following description of a particular embodiment given by way of non limiting example, and which refers, additionally to the above mentioned figures showing the prior art, to the accompanying drawings in which :

- Figures 1 and 2, already mentioned, are schematic drawings figuring the architecture of the PIN code interface of the prior art.

- Figure 3 is a schematic drawing showing the architecture of the system according to the present invention.

- Figure 4 is a schematic drawing showing an interactive television system for implementing the invention.

- Figure 5 is a flowchart related to the application according to the embodiment of the invention more particularly described here.

- Figure 6 is a flowchart implemented by the security manager means according to the embodiment of the invention more particularly described here.

Figure 3 shows a system 10 arranged to authenticate the user before running an application 11, according to the invention.

The application 11 initiates a PIN entry request 12 to authenticate the user request and simultaneously asks the security manager means 13 to handle key input 14 to be introduced through Input means 15, for instance through a key pad.

The security manager means 13 comprises a small computer system including a central processing unit (CPU), memory and local storage. It is connected to input/output ports.

It is programmed in order to provide the different steps according to the method of the invention.

The application having total control over the graphics displayed and their look and feel, the look

and feel 16 for PIN entry is provided on display means 17 according to the application.

The display means can be a TV screen, an LCD screen of a remote portable telephone, etc.

As the security manager means 13 is asked to enter the PIN entry mode, it grabs key inputs 14, analyses these inputs for user authentication and relays in 18 the key presses to the application.

The security manager means does not relay the key values, which therefore remains within the system, but only relays the fact that a key has been pressed, letting for instance the application display an X for each key pressed, in the PIN entry field.

This way the application does not learn about the PIN, but can give user feedback 19 to the display means 17.

When the security manager means 13 recognises the PIN, it informs in 20 the application that the user/viewer has been authenticated.

The application can then run, be displayed and/or operate.

Figure 4 shows schematically an interactive television system 21 including a system S according to the embodiment of the invention more particularly described here.

A broadcaster 22 transmit through a satellite 23 the signal corresponding to the look and feel of an application request (arrows 24), for instance a Pay TV program.

The signal is provided to a digital interactive decoder 25, currently packaged in a set-top connected to a television 26.

It delivers true interactive television using the broadcast-oriented infrastructure currently predominant in the television industry.

The decoder 25 comprises in a manner known per se, a demultiplexer 27 and an application programming interface 28, stored in a local memory (RAM, EPROM FLASH memory, ...), such as the one proposed by the applicant OPEN TV, and which provides a library of functions which can display graphics on the television screen, control audio/video services, accept user input and communicate with the outside world.

The decoder 25 also comprises a CPU 29, Audio/Video decoding means 30, connected through audio video output 31 to the television set 26, storage means 32 for storing an operating system for the CPU 29, such as the one provided by OPEN TV.

The CPU 29 further includes part of the security manager means 33 as described in the invention.

The decoder 25 also comprises Input means 34 such as infrared sensors arranged to receive infrared signals 35 emitted by a remote control apparatus 36 having a key pad 37, and display function means 38 controlled by the CPU.

The decoder 25 also comprises output means having a modem and/or a multiplexer 39 for providing back return signals 40 on a return channel to the broadcaster 22 and/or a server.

The broadcast system may be, of course based on satellite or cable or some other medium.

Figure 5 shows a block diagram according to an embodiment of the invention to be included in an application to authenticate the users to continue or to have access to specific resources which needs authentication by a PIN code.

The application first uses some display function (block 41) to present a PIN entry field to the viewer.

It then asks the security manager means to enter the PIN entry mode and check in 43 if keys are pressed.

As keys are pressed, it gives (block 44) feedback using the display function.

If the user is not authenticated (step 45), it comes back (loop 46) to check 43.

If the user is authenticated (in 47), there is an OK from the security manager means and the application can go on (step 48).

An example of a block diagram of the security manager program is provided on figure 6 and is performed entirely (and secretly) within the System S.

At the application request in 49, the security manager means enters a PIN entry mode (step 50).

The PIN repertory is then initialised to empty in 51 and the system wait for a key to be pressed (check 52).

If the key is an « ending » key (for instance OK or enter), (check 53) there is a release of the key input grabbing (step 54).

If not there is a loop 55 for more key.

After release of the key input grabbing, the security manager means checks in 56 the entered PIN against the user's PIN.

It then either returns success (step 57), or failure (step 58) to application (step 45 of the application), before exiting PIN entry mode in 59.

It will now be described the functioning of the system while referring to figure 4.

At the broadcast site, pay TV programs of a Specific Provider are stored.

The pay TV programs are encoded into a digital bitstream which is compressed and multiplexed with the signal of the PIN code field of the Specific Provider, including its logo and a menu to allow the viewer to have access to other movies of the provider, to form a single bitstream.

This single bitstream is then broadcasted to all subscribers. At each customer's site, the bitstream is received by the decoder 25 where the audio and video are decompressed and the PIN code field is sent to the customer's television set 26.

The request for the PIN code of the user is therefore prompted to the viewer.

The viewer then, for instance through a remote control apparatus, can enter his PIN code by pressing keys.

At each pressing, a cross appears in the PIN entry field on the TV Screen.

Meanwhile the Security manager means 33 compares the PIN code with a preregistered user's PIN code entered before in the decoder for instance via a modem.

If the PIN codes matches, signals are sent to the application decoding process 30, and such deccding process is then authorised for displaying the application on the TV set.

Additional advantages and modifications will readily occur to those skilled in the art. Therefore the present invention in its broader aspects is not limited to the specific details, representative devices and illustrated examples shown and described herein.

For instance, it also includes application to PIN code entry for obtaining specific services through mobile phone, for instance via GSM, or other specific services via Television and/or Internet.

CLAIMS

1. A system (10, S) for authenticating a PIN code of a user in an interactive information system in order to run an application (11),
wherein it comprises
- input means (15, 34, 35, 36, 37) for PIN code entry,
- security manager means (13, 33) for comparing the PIN code of the user upon a request for user authentication from the application, with a registered PIN code, and giving authorisation to run said application if the PIN code of the user matches with the registered PIN code, and
- display means (17, 29, 38) for displaying any graphics including a PIN entry field,
characterised in that
the request for user authentication being provided on the display means via the Pin entry field with the look and feel of said application, the system further comprises emitting means (29, 38) for entering crypted digits in said PIN entry field upon entering the PIN code of the user in the security manager means through said input means,
and the security manager means (13, 33) are arranged to give authorisation to run the application after full entry of said crypted digits and if the PIN code of the user is identical to the registered PIN code.

2. A system according to claim 1 characterised in that the application is a television program.

3. A system according to claim 1, characterised in that the application is a service provided on mobile Telephone.

4. A method for authenticating a PIN code of a user in an interactive information system, in order to run an application,
wherein said information system emits a request for authenticating a user (41),
said user enters a PIN code (43) through input means,
said PIN code of the user is compared (45) with a registered PIN code within security manager means,
and authorisation is provided to run said application if the PIN code of the user matches with the registered PIN code,
characterised in that
- the request for authenticating being provided with a PIN entry field having the look and feel of the application,
- crypted digits are entered (44) in said PIN entry field, upon entering the PIN code by the user in the security manager means,
and authorisation to display the application is only provided (47) after full entry of said crypted digits, and if the PIN code of the user is identical to the registered PIN code as checked by the security manager means.

5. A method according to claim 4, characterised in that, for presenting the request for authentication, the application undertakes the following steps :

- presenting a PIN entry field to the user (41),
- asking the security manager means to enter a PIN Entry Mode (42),
- the input means comprising keys, checking if keys are pressed by the user (43),
- while keys are pressed, giving feedback in entering said crypted digits in said PIN entry field (44), and,
- if the user is authenticated (45) by said security manager means, giving said authorisation (47) to display (48) the application.

6. A method according to any of claims 4 and 5, characterised in that, for providing the authorisation to display the application the security manager means undertakes the following steps :

- at the request of the application entering a PIN entry mode (50),
- initialising to empty a PIN repertory (51) and, the input means comprising keys, waiting for a key to be pressed by the user (52),
- upon occurrence of pressing an « ending key », checking if a release occurs (53), checking the entered PIN against the user's PIN (56), and if success authorising the application to run.

7. A method according to any of claims 4 to 6, characterised in that the application is a Television program.

8. A method according to any of claims 4 to 6, characterised in that the application is a service provided on a mobile telephone.

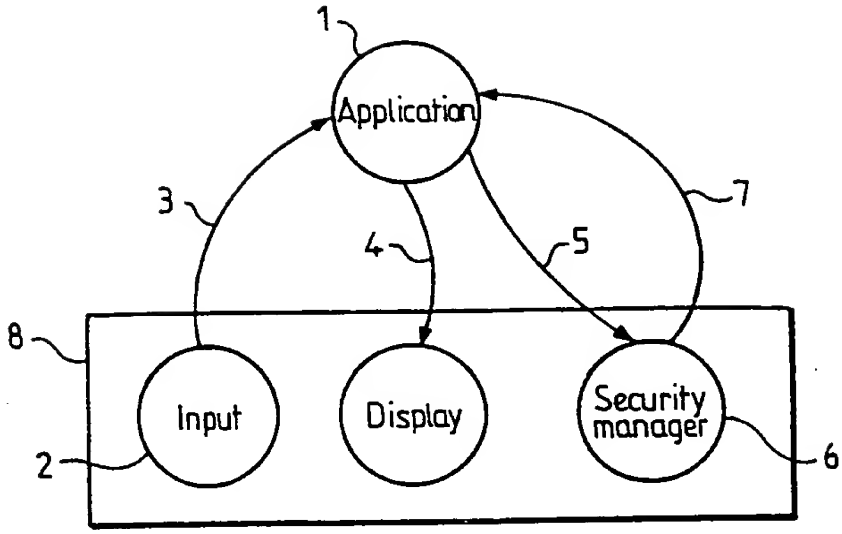


FIG.1 PRIOR ART

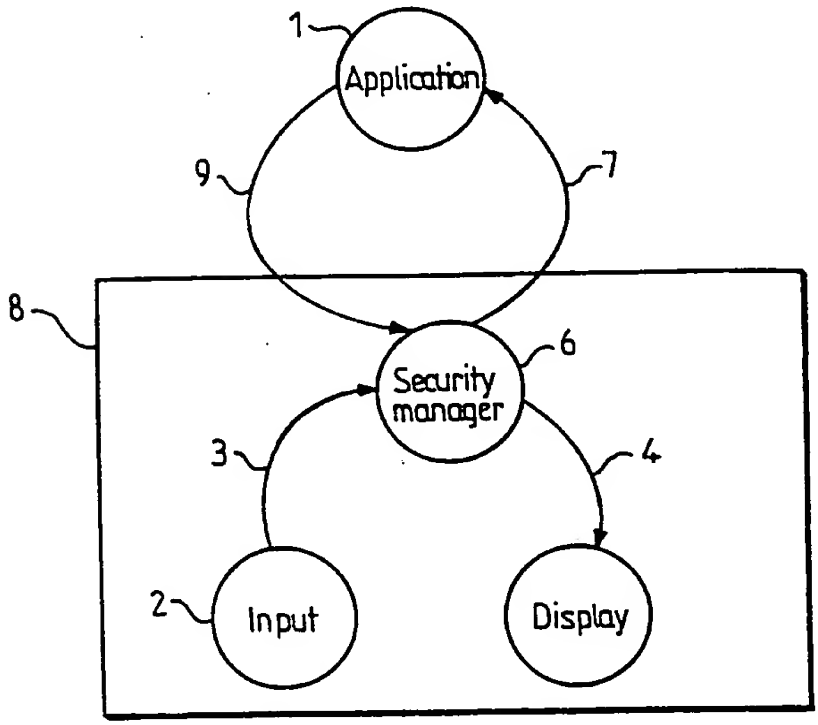


FIG.2 PRIOR ART

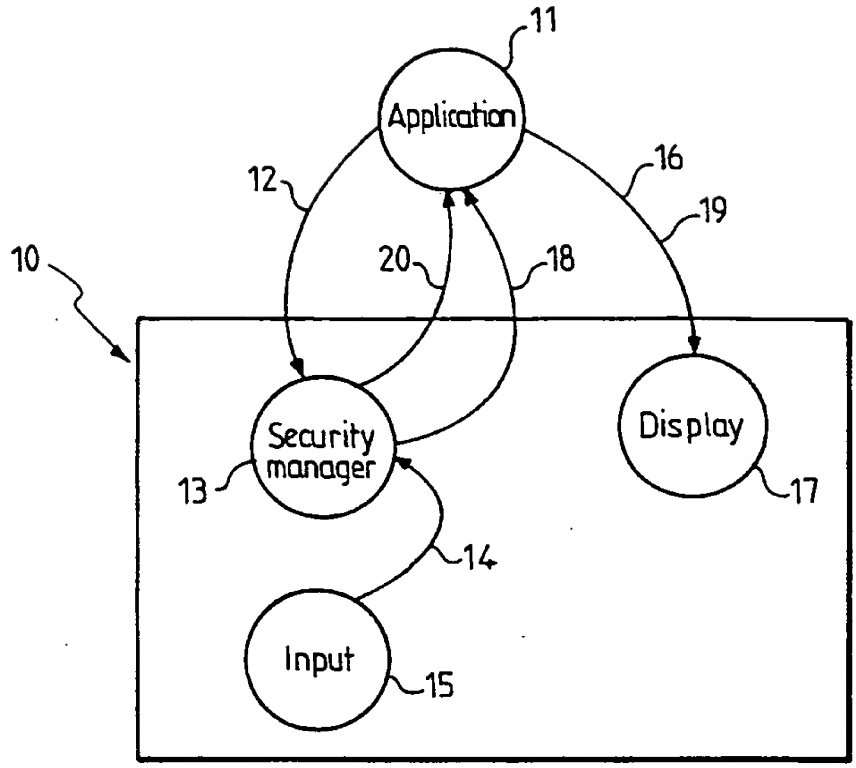

11
Application
12
16
19
10
20
18
Security manager
13
Display
17
14
Input
15

FIG. 3

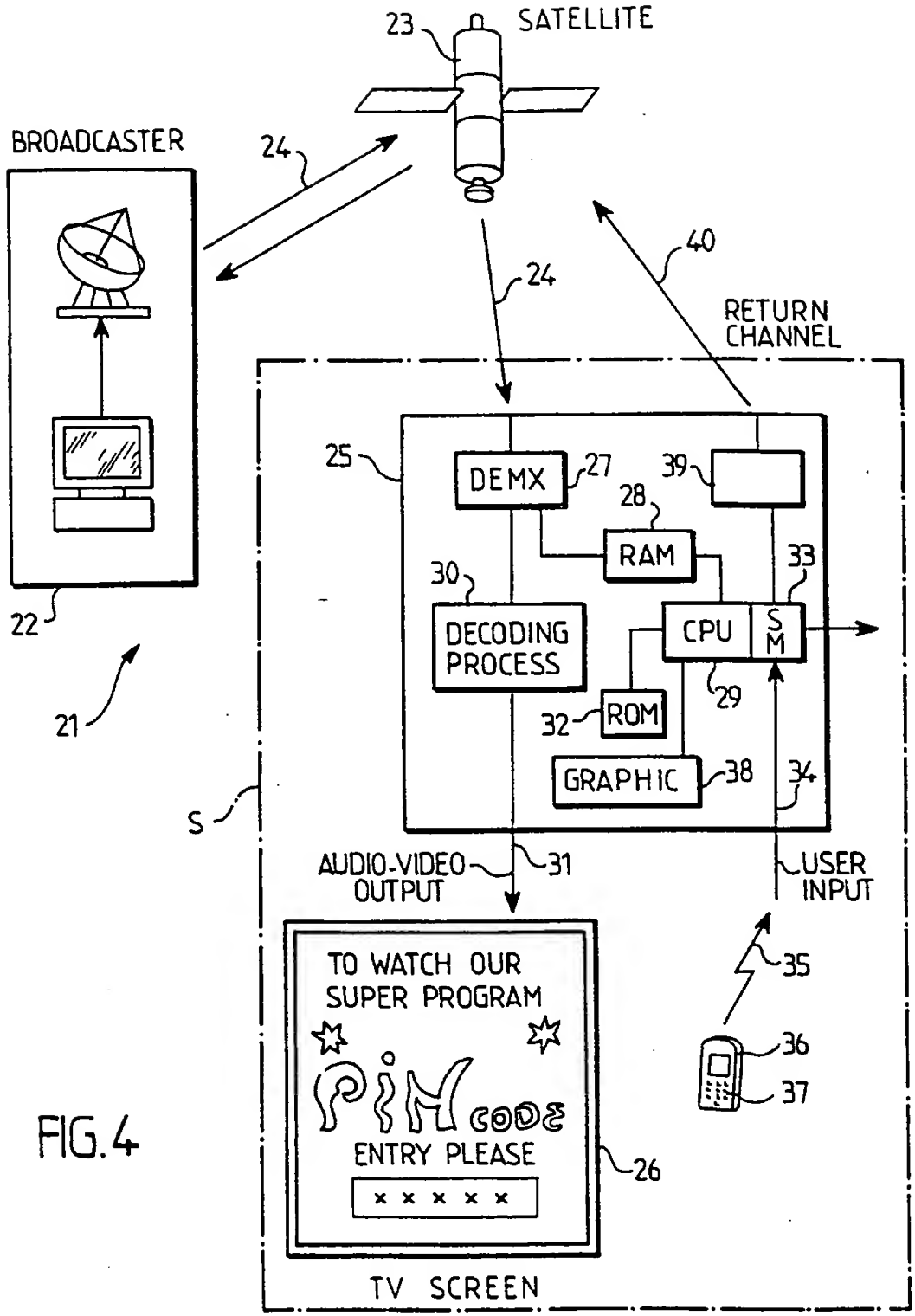

23
SATELLITE
BROADCASTER
24
24
40
RETURN CHANNEL
25
DEMX
27
39
28
RAM
33
30
DECODING PROCESS
CPU
S M
29
32
ROM
GRAPHIC
38
34
22
21
S
AUDIO-VIDEO OUTPUT
31
USER INPUT
TO WATCH OUR SUPER PROGRAM
PIN CODE
ENTRY PLEASE
× × × × ×
26
35
36
37
TV SCREEN

FIG.4

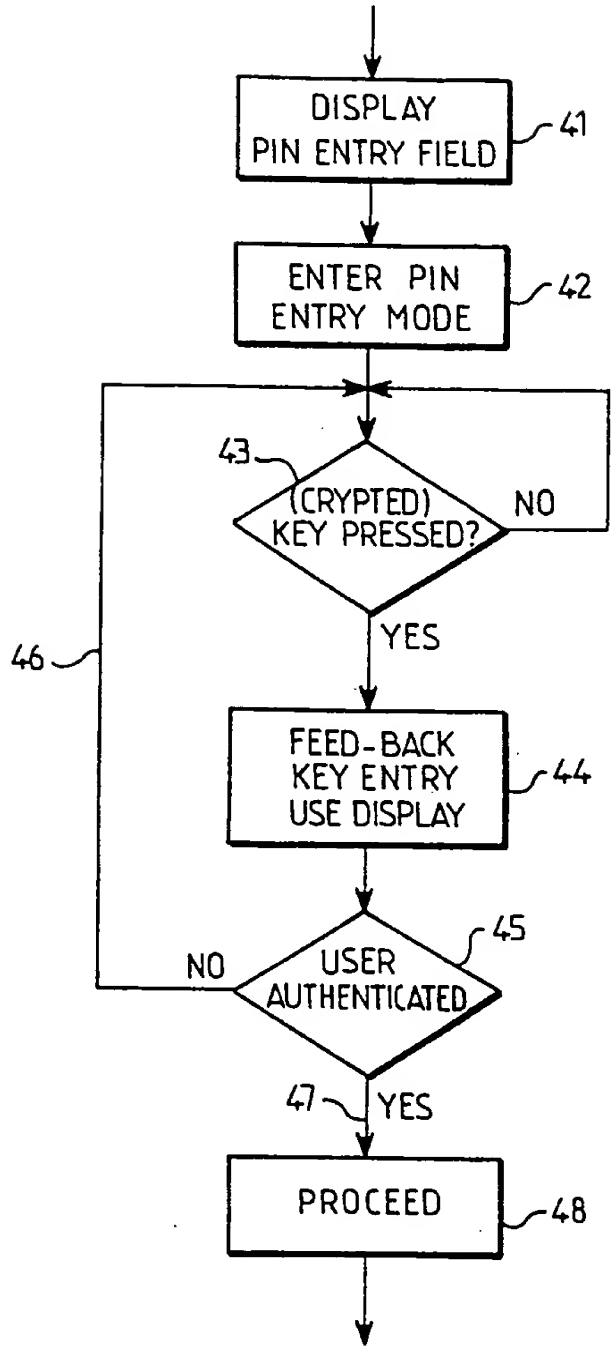

DISPLAY PIN ENTRY FIELD
41
ENTER PIN ENTRY MODE
42
43
(CRYPTED) KEY PRESSED?
NO
YES
46
FEED-BACK KEY ENTRY USE DISPLAY
44
45
NO
USER AUTHENTICATED
47
YES
PROCEED
48

FIG.5

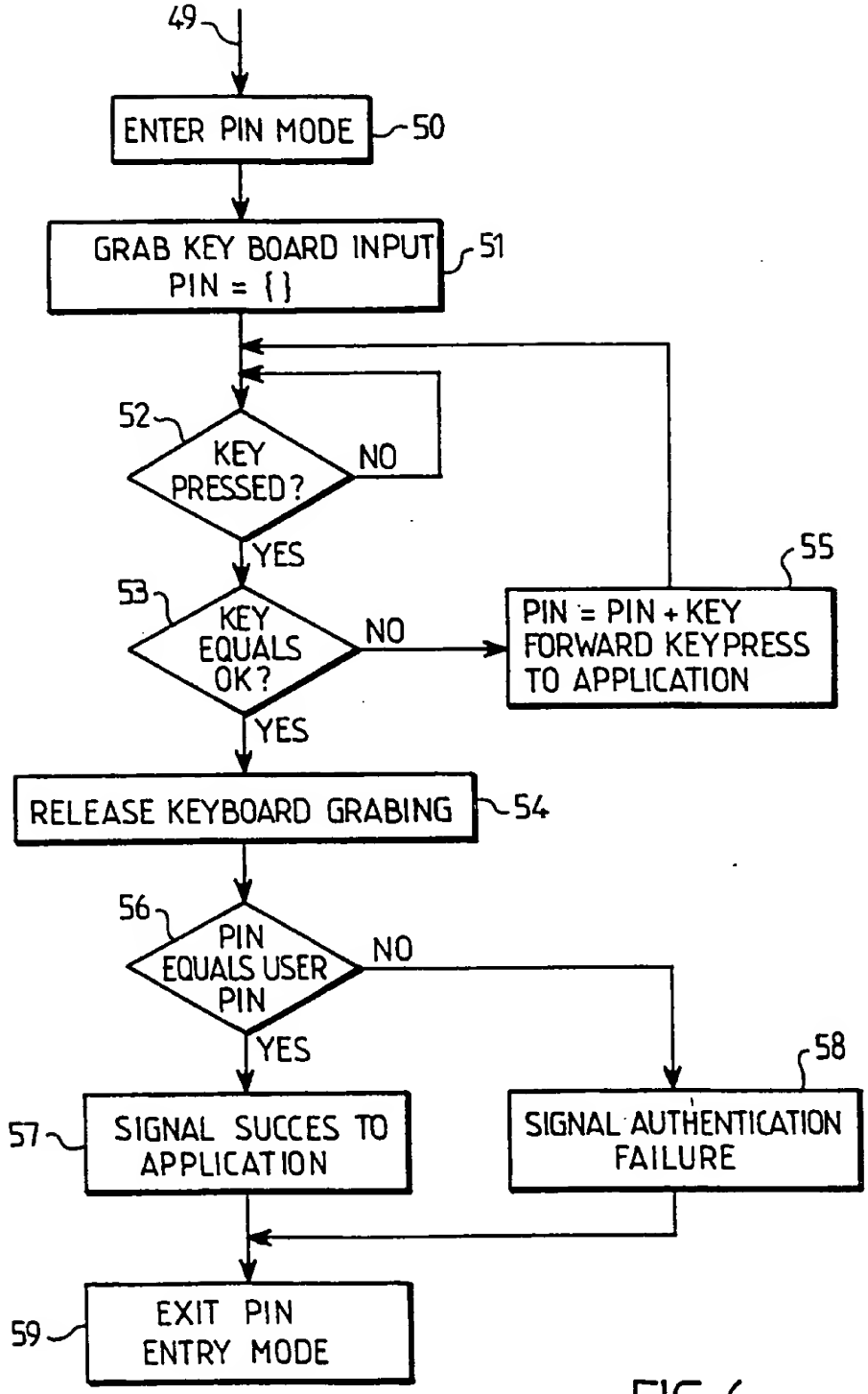

49
ENTER PIN MODE
50
GRAB KEY BOARD INPUT
PIN = { }
51
52
KEY PRESSED?
NO
YES
53
KEY EQUALS OK?
NO
55
PIN = PIN + KEY
FORWARD KEYPRESS
TO APPLICATION
YES
RELEASE KEYBOARD GRABING
54
56
PIN EQUALS USER PIN
NO
YES
58
57
SIGNAL SUCCES TO APPLICATION
SIGNAL AUTHENTICATION FAILURE
59
EXIT PIN ENTRY MODE

FIG.6

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/IB 99/01213

A. CLASSIFICATION OF SUBJE ATTER
IPC 7 H04N7/16 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04N G07F H04L H04Q G06F G07C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 870 723 A (HOFFMAN NED ET AL) 9 February 1999 (1999-02-09) column 4, line 28 - line 49 column 10, line 1 - line 7 column 16, line 19 - line 29 ---	1-8
Y	US 5 682 325 A (GOODMAN WILLIAM ET AL) 28 October 1997 (1997-10-28) abstract column 15, line 41 -column 16, line 44 ---	1,2,4,5, 7
Y	US 5 267 149 A (ANADA NORIAKI ET AL) 30 November 1993 (1993-11-30) figure 3B column 3, line 50 - line 55 column 4, line 34 - line 51 --- -/--	1,2,4,5, 7

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
8 February 2000	15/02/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Lindholm, A-M

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS [redacted]IDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 98 37695 A (SCIENTIFIC ATLANTA ;TIME WARNER ENTERTAINMENT COMP (US)) 27 August 1998 (1998-08-27) page 62, line 10 - line 34; figure 25 ---	1
A	WO 97 19555 A (PREVUE INTERNATIONAL INC) 29 May 1997 (1997-05-29) figures 2,5 page 1, line 24 -page 2, line 2 page 2, line 24 - line 30 page 10, line 1 - line 9 ---	1,2,4-7
A	EP 0 564 832 A (IBM) 13 October 1993 (1993-10-13) column 6, line 41 - line 55; figure 4 ---	6
A	WO 98 00968 A (FCA CORP DOING BUSINESS AS FOR) 8 January 1998 (1998-01-08) page 10, line 14 - line 21 ---	6
A	US 4 947 429 A (BESTLER CHARLES B ET AL) 7 August 1990 (1990-08-07) abstract column 1, line 54 - line 64 column 3, line 1 - line 22 -----	1

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter nal Application No
PCT/IB 99/01213

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5870723 A	09-02-1999	US 5613012 A	18-03-1997
		US 5615277 A	25-03-1997
		AU 4329597 A	19-03-1998
		WO 9809227 A	05-03-1998
		US 6012039 A	04-01-2000
		AU 5922696 A	29-11-1996
		BR 9608580 A	05-01-1999
		CA 2221321 A	21-11-1996
		CN 1191027 A	19-08-1998
		EP 0912959 A	06-05-1999
		JP 11511882 T	12-10-1999
		WO 9636934 A	21-11-1996
		US 5838812 A	17-11-1998
		US 5764789 A	09-06-1998
		US 5802199 A	01-09-1998
		US 5805719 A	08-09-1997
US 5682325 A	28-10-1997	US 5740075 A	14-04-1998
		US 5621728 A	15-04-1997
		US 5748493 A	05-05-1998
		US 5917537 A	29-06-1999
US 5267149 A	30-11-1993	JP 63174172 A	18-07-1988
		JP 63178381 A	22-07-1988
		JP 63049971 A	02-03-1988
		KR 9105350 B	25-07-1991
WO 9837695 A	27-08-1998	US 5850218 A	15-12-1998
		AU 6176298 A	09-09-1998
		AU 6176398 A	09-09-1998
		EP 0962096 A	08-12-1999
		WO 9837694 A	27-08-1998
WO 9719555 A	29-05-1997	AU 707081 B	01-07-1999
		AU 1021797 A	11-06-1997
		BR 9611743 A	23-02-1999
		EP 0862833 A	09-09-1998
EP 0564832 A	13-10-1993	US 5276314 A	04-01-1994
		CA 2089306 A,C	04-10-1993
		JP 2837784 B	16-12-1998
		JP 6083777 A	25-03-1994
WO 9800968 A	08-01-1998	US 5973756 A	26-10-1999
		AU 3957397 A	21-01-1998
		EP 0906691 A	07-04-1999
US 4947429 A	07-08-1990	NONE	